HACS - ACES-CYBERSECURITY

HACS408 Advanced Seminar in Cybersecurity (3 Credits)
Explores various lenses of cybersecurity in order to promote an interdisciplinary understanding of the field. Although each section may focus on a different topic, each integrates active student engagement, communication, critical communication, critical thinking, and teamwork.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.
Repeatable to: 9 credits if content differs.

HACS408C Interpersonal Cyber Communications (3 Credits)
Designed to prepare students to participate in culturally responsible and environmentally appropriate communication in the workforce. Students will explore the industry standards for writing technical reports, as well as the variances between persuasive, team, written, and oral communication styles.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408L Analytical and Forensic Techniques for Cybersecurity (3 Credits)
Explores forensic artifacts contained in digital devices, security mechanisms available to protect digital devices and mechanisms available to cybersecurity professionals for analysis of digital devices. Topics include file structure and recovery of IoT and cell phone forensic data, network data capture and analysis, enterprise mobile device management analysis and forensic investigation of digital devices (IoT, telematics systems, etc.) that interact with cell phone and other devices. Incident response, timeline analysis, and detection and analysis of artifacts will be explored in a hands-on and lab-centric course using a variety of open-source tools and commercial cloud services.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408M Introduction to Cyber Threats and Risk Management (3 Credits)
Provides an exploration of cyber risk management and present-day cyber threats, their impacts, and their mitigations. Students will take a multi-disciplinary approach to understanding threats and risks including the technical, policy, and social aspects. This course is guided by real-world cyber threats and examples.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408O Internet of Things Security (3 Credits)
This increasingly interconnected world brings a need for understanding cybersecurity challenges associated with embedded devices and systems. This course will expose students to topics in Internet of Things (IoT) and Cyber Physical System (CPS) device types, IoT/CPS threat categories, security services, distributed networking, activity privacy, and intrusion detection for embedded environments. In addition to individual homework assignments, students will participate in a semester long group project involving research, design, and implementation.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408T Penetration Testing (3 Credits)
A hands-on, technically rigorous experience that prepares students for real-world work in penetration testing and offensive security. This course will allow students to gain proficiency and become comfortable using the tools, techniques, and methodologies that represent the state of the art in penetration testing today. Students should be comfortable on the command line, and a technical exposure to networking and basic proficiency in some scripting language (Bash, Ruby, or Python) is expected.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408V Data Analysis and Visualization for Cybersecurity (3 Credits)
Focuses on exploratory and statistical data analysis, data and information visualization, and the presentation and communication of analysis results. These topics will be presented and explored in the context of and with applications to cyber security related data. Examples and illustrations will often involve the R programming language, but prior experience with R is not required and submitted work may involve the use of other languages and tools at times.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS479 Undergraduate Research in Cybersecurity (1-3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in research in order to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and to prepare for graduate school and the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.
Repeatable to: 6 credits if content differs.

HACS487 Undergraduate Research in Cybersecurity (3 Credits)
A semester-long, individualized academic research project. Students work with a faculty supervisor to design and research an original topic. Students engage in research to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and prepare for graduate school and/or the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.

HACS497 Cybersecurity Experience Reflection (3 Credits)
Cybersecurity experience is defined as an experiential learning activity either with a University of Maryland entity or with an external organization that will provide valuable, hands-on experience to supplement the knowledge learned in other ACES coursework. This course is intended to help students reflect on their cybersecurity experience and to learn from others' cybersecurity experiences. It is also intended to help students gain professional skills that will aid in their future career.
Prerequisite: Students may enroll concurrently with or after completing a cybersecurity related internship experience of at least 135 hours.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and must not have taken HACS297.
Credit Only Granted for: HACS297 or HACS497.

HACS498 Cybersecurity Group Problem Solving (3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in team problem solving activities in order to gain greater insight into a specific area within cybersecurity and to obtain an appreciation for the subtleties and difficulties associated with these activities in order to prepare students for graduate school and the workforce. Students engage in a semester long problem solving or development project under the mentorship of a industry specialist and with the guidance of university faculty. Through the exercise the students will develop teamwork experience and professional communication skills in addition to experience of the project itself. The project might be evaluation, creation, testing or analysis of some area of cybersecurity as needed by the mentor-sponsor. A contract of what will be accomplished is required must be agreed upon by the mentor, the student and the ACES leadership before the project can begin.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.
Repeatable to: 6 credits.